TASK ORDER AWARD
47QFCA20F0049 - P00000

United States Southern Command (USSOUTHCOM) Cyber Information Technology Enterprise Services (SCITES)

in support of:

USSOUTHCOM

Issued to:
GDIT
3150 Fairview Park Drive
Falls Church, VA 22042

Awarded under (GSA) Alliant 2
Government-wide Acquisition Contract #47QTCK18D0003
Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

September 25, 2020
FEDSIM Project Number DE01093

C.1 BACKGROUND

The United States Southern Command (USSOUTHCOM) J6 United States Army Network Enterprise Center (J6/USANEC) is tasked by the Combatant Commander to implement and sustain United States (U.S.) and partner nation Information Technology (IT) to enable full-spectrum operations in the USSOUTHCOM Area of Responsibility (AOR), which consists of Central America, South America, and select countries in the Caribbean. In addition, United States Cyber Command (USCYBERCOM) has Directive Authority for Cyber Operations (DACO) on USSOUTHCOM's constructed networks (AO Uniform), and USSOUTHCOM must comply with Cyber Task Orders under DACO.

C.1.1 PURPOSE

USSOUTHCOM requires centralized IT infrastructure, services, and processes to include Cybersecurity Task Order (CTO) compliance activities for the USSOUTHCOM AO Uniform constructed networks. This includes three enduring Joint Task Forces (JTFs) and multiple Security Cooperation Office(s) (SCO). USSOUTHCOM must have the ability to Command and Control (C2) CTO and network management activities for AO Uniform from a Network Operations and Security Center (NOSC), located at HQ, encompassing Tier 3 Cyber Security Service Provider (CSSP) capabilities. These capabilities are required to meet the USSOUTHCOM's mission and those of its various mission partners, to include, but not limited to, other Department of Defense (DoD) organizations, other U.S. Federal and state government agencies, and foreign government military and non-military mission partners.

C.1.2 AGENCY MISSION

USSOUTHCOM deters aggression, defeats threats, rapidly responds to crises, and builds regional capacity, working with our allies, partner nations, and U.S. Government (USG) team members to enhance security and defend the U.S. homeland and its national interests. USSOUTHCOM is responsible for providing contingency planning, operations, and security cooperation in its assigned AOR which includes Central America, South America, and the Caribbean (except U.S. commonwealths, territories, and possessions). The Command is also responsible for the force protection of U.S. military resources at these locations. USSOUTHCOM is responsible for ensuring the defense of the Panama Canal. Under the leadership of a four-star commander, USSOUTHCOM's staff is organized into directorates, component commands, and SCOs that represent USSOUTHCOM in the region. USSOUTHCOM is a joint command comprised of more than 1,200 military and civilian personnel representing the Army, Navy, Air Force, Marine Corps, Coast Guard, and several other Federal agencies. The services provide USSOUTHCOM with component commands which, along with their Joint Special Operations component, two JTFs, one Joint Interagency Task Force, and SCOs, perform USSOUTHCOM missions and security cooperation activities. USSOUTHCOM exercises its Combatant Command authority through the commanders of its components, JTFs/Joint Interagency Task Force, and SCOs.

C.2 SCOPE

The scope of this effort includes program management services, transition services, and a full range of enterprise IT-related services and technical solutions that span cybersecurity and IT

management. These enterprise IT-related services will be directed by an AO Uniform NOSC to coordinate operations, data transport, compliance, personnel security, projects, integration, engineering, logistics, and sustainment of USSOUTHCOM mission.

The scope includes establishing and maintaining a program of AO Uniform environment-wide IT, CSSP, and Defensive Cyber Operations for AO Uniform constructed networks. AO Uniform environment-wide IT, CSSP and Defensive Cyber Operations shall provide secure, available, seamless, effective, and efficient cyber and IT services, which prioritize the reduction of IT risk to the Combatant Commander. In addition, the contractor shall provide IT lifecycle services efforts across the AOR. This requirement is to create a system of systems architecture consisting of open-standard, open-architecture, Commercial Off-the-Shelf (COTS) and/or Government Off-the-Shelf (GOTS) hardware and software services capable of operating in global environments. This requirement shall deliver enterprise class, industry standard, open-architecture, and open-standards equipment and services to USSOUTHCOM.

USSOUTHCOM requires a wide range of technologies that include, but are not limited to, installation; Operations and Maintenance (O&M) of a Tier 3 CSSP system of systems and infrastructure; cloud computing; edge computing; and multiple X as a Service (XaaS) solutions. XaaS solutions are those such as Software as a Service (SaaS), Desktop as a Service (DaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) as well as others. DaaS is normally defined as some type of Virtual Desktop Interface (VDI) including, but not limited to, thick client, thin client, and zero client type solutions as well as web-based VDI front ends. USSOUTHCOM requires Tier 1 through Tier 4 IT services; multiple methodologies of software development including, but not limited to, Agile software development as well as employment of principles and elements of DevSecOps; expertise in developing, deploying, and maintaining a system of systems of IT infrastructure; and making use of elements and principles of Defense Enterprise Service Management Framework (DESMF). Providing services and equipment in this environment also requires an in-depth knowledge of mission-specific operational requirements for multiple mission partners leveraged in multiple geographical locations including Continental United States (CONUS) and Outside the Continental United States (OCONUS). This requirement includes designing, transitioning, and operating all network services in accordance with Joint Information Environment (JIE) standards and Defensive Cyber Operations.

Additionally, this scope includes research, engineering, integration, and O&M of new capabilities across the AOR. This includes, but is not limited to, identifying, researching, testing, and recommending emergent technologies to meet identified USSOUTHCOM capability gaps, Government- and DoD-mandated improvements, strategic directives, and advances in technology and security. It also includes assisting in the down selecting of technologies based on capabilities, cost, interoperability, and other factors for implementation into the AO Uniform environment.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

USSOUTHCOM IT consists of several combatant command constructed networks across an AO that includes the portions of the U.S., South America, Central America, and the Caribbean. USCYBERCOM has DACO and issues CTOs to USSOUTHCOM for compliance activities. IT operations and management, to include limited CTO compliance activities, is currently accomplished by a decentralized, traditional (legacy) IT operations model.

C.4 OBJECTIVE

The objectives of the SCITES Task Order (TO) include the following:

a. Establish an NOSC.
b. Transition to AO Uniform construct.
c. Transition from IPv4 to IPv6.
d. Virtualization and cloud migration.
e. Innovation and incorporation of emergent technologies.
f. Increased efficiencies in Operations and Maintenance (O&M) spending.

C.4.1 ESTABLISH A NETWORK OPERATIONS AND SECURITY CENTER (NOSC)

USSOUTHCOM seeks to establish a NOSC with Tier III CSSP capabilities through the installation and O&M of an open standard and open architecture system of systems and related infrastructure. This shall be accomplished by aligning Defensive Cyber Operations and IT Service Operation under a single consolidated umbrella for the AO Uniform and integrating capabilities with USSOUTHCOM NOSC. The integration and employment of cybersecurity activities for Department of Defense Information Network (DODIN) operations with internal defensive cyber operation measures in response to vulnerabilities and threats shall reduce risk across the USSOUTHCOM cyber battlefield. Further, by migrating appropriate end-point devices and client-based applications to VDI and SaaS models, USSOUTHCOM will be able to more rapidly respond to tasks and objectives issued from the authorities of USCYBERCOM DACO and USSOUTHCOM DACO over USSOUTHCOM-constructed networks.

C.4.2 TRANSITION TO AO UNIFORM CONSTRUCT

USSOUTHCOM is transitioning from multiple, disparate, geographically separated networks to a unified construct that is referred to as AO Uniform. To reach this objective, USSOUTHCOM seeks to develop, integrate, operate, and maintain IaaS throughout the AO Uniform environment. The Joint Regional Security Stack (JRSS) is a currently supported IaaS critical component for creating such environments because it centralizes and modernizes the transport and defensive capabilities needed to defend the USSOUTHCOM enterprise. The objective AO Uniform environment shall be an open standards and open architecture IaaS environment (JRSS compliant) for all supported networks and infrastructures.

C.4.3 TRANSITION FROM IPV4 TO IPV6

USSOUTHCOM needs to transition the current IPv4-constructed networks to a pure IPv6 network environment. To meet this objective, USSOUTHCOM is seeking design, development, engineering, and deployment services for a new hardware and software infrastructure. The new designs shall be open standards and open architecture compliant. During the transition period, the infrastructure shall provide a dual-stack environment capable of handling both IPv4 and IPv6 simultaneously while maintaining or reducing the operational risk to AO Uniform.

C.4.4 VIRTUALIZATION AND CLOUD MIGRATION

USSOUTHCOM is seeking to virtualize and migrate select applications and data to the cloud in order to better support mission applications and allow the enterprise to benefit from modern, cloud-native characteristics such as rapid deployment, dynamic provisioning, and resource

pooling. The cloud repository technologies that shall be supported include on-premise, hybrid, and public and private clouds. Applications that are migrated to an infrastructure based in the cloud, connected by software-defined networks deliver flexible, mobile, and secure access to data and analytics, and shall provide the resiliency and elastic capacity necessary to achieve the performance expected of large-scale applications at a reasonable cost. Additionally, cloud migration leads to Continuity of Operations (COOP) improvements as well as Disaster Recovery (DR) improvements.

C.4.5 INNOVATION AND INCORPORATION OF EMERGENT TECHNOLOGIES

USSOUTHCOM's portfolio of systems, systems of systems, dependencies, and support requires careful and methodical balance between performance, dependency, buying down technical debt, supporting various missions, and new functionality or systems development. To attain this, USSOUTHCOM is continually seeking identification of innovative approaches and emergent technologies to be more effective at IT portfolio delivery, management, and governance, leading to the more efficient allocation of resources, a better coordinated development and release process, and a more predictable security and Authorization to Operate (ATO) process. Through identifying, researching, testing, and recommending emergent technologies to meet identified USSOUTHCOM capability gaps, Government- and DoD-mandated improvements, strategic directives, and advances in technology and security, USSOUTHCOM aims to reduce technical debt and improve mission effectiveness. These goals are also accomplished via the down selecting of technologies based on capabilities, cost, interoperability, and other factors for implementation into the AO Uniform environment.

C.4.6 INCREASED EFFECIENCIES IN OPERATIONS AND MAINTENANCE (O&M) SPENDING

Over the past decade the number of systems in the USSOUTHCOM portfolio has risen due to operational, mission and other statutory and regulatory requirements. Many of these systems are legacy or duplicative and do not align with the future-state objectives. USSOUTHCOM is seeking an approach to reduce its IT footprint and optimize O&M spending through modernization, re-architecture, or other service oriented approaches. While no sustainment reduction cost targets have been defined, the contractor shall seek opportunities to reduce long-term spending through elimination of duplicative capabilities and high sustainment cost constructs.

C.5 TASKS

The associated tasks with this scope are:

Task 1 - Provide Task Order (TO) Management

Task 2 - Transition Services

Task 3 - Operations Services

Task 4 - Transport Services

Task 5 - AO Uniform Constructed NOSC Services

Task 6 - Compliance and Personnel Security Services

Task 7 - Projects, Integration, and Engineering (PIE) Services

Task 8 - Logistics Services

Task 9 - Additional USSOUTHCOM Cyber Information Technology Enterprise Services (SCITES) Augmented Services (Optional)

The offer shall provide IT Tier 1 through Tier 4 services. Below are the definitions for IT Tier Service as they pertain to the Tasks and Subtasks in this TO.

a. **IT Tier 1 Service –** The initial service level responsible for basic customer issues. It is synonymous with first-line service, level 1 service, front-end service, and various other headings denoting basic-level technical functions. The first job of a Tier 1 service individual is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem. When analyzing the symptoms, it is important for the Tier 1 individual to identify what the customer is trying to accomplish so that time is not wasted on attempting to solve a symptom instead of a problem. If the problem cannot be solved at this level due to complexity or lack of permissions, the problem is elevated to the next Tier.

b. **IT Tier 2 Service –** A more in-depth technical service level than Tier I, and the technicians are more experienced and knowledgeable on a particular product or service. It is synonymous with level 2 service, service line 2, administrative-level service, and various other headings denoting advanced technical troubleshooting and analysis methods. Technicians in this realm of knowledge are responsible for assisting Tier I personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues. This team usually collects information such as program name that failed, application name, or any database-related details (e.g., table name, view name, package name) or Application Programming Interface (API) names. If the problem cannot be solved at this level due to complexity or lack of permissions, then the problem is elevated to the next tier.

c. **IT Tier 3 Service –** Typically the highest level of services in a three-tiered technical service model responsible for handling the most difficult or advanced problems. These individuals are experts in their fields and are responsible for not only assisting both Tier I and Tier II personnel, but with the research and development of solutions to new or unknown issues. This team can analyze the code and data using information from Tiers 1 and 2. In some instances, an issue may be so problematic to the point where the product cannot be salvaged and must be replaced. Such extreme problems are also sent to the original developers for in-depth analysis. If it is determined that a problem can be solved, then this group is responsible for designing and developing one or more courses of action, evaluating each of these courses in a test-case environment, and implementing the best solution to the problem. Once the solution is verified, it is delivered to the customer and made available for future troubleshooting and analysis. If the problem cannot be solved at this level due to complexity or lack of permissions, the problem is elevated to the next tier.

d. **IT Tier 4 Service –** While not often used, a fourth level represents an escalation point beyond the normal O&M organization. This is either systems engineering (responsible

for implementing new capabilities) or generally a hardware or software consulting vendor or hardware or software Original Equipment Manufacturer (OEM) Field Engineer.

e. **After Hour/On Call and Holidays –** The contractor shall provide a one-hour response time and be onsite within two hours to IT related incidents or concerns at USSOUTHCOM HQ and JTFs and SCOs with permanent personnel. For SCOs without permanent on-site support, the contractor shall provide 24-hour response time, country clearance process permitting.

C.5.1 TASK 1 – PROVIDE TASK ORDER (TO) MANAGEMENT

The contractor shall provide TO management services under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1.1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs shall be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the aforementioned website.

C.5.1.2 SUBTASK 1.2 – COORDINATE A PROGRAM KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Program Kick-Off Meeting (**Section F, Deliverable 02**) at the location approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, USSOUTHCOM Government Representatives and Stakeholders, the USSOUTHCOM Technical Point of Contact (TPOC), FEDSIM CO, the FEDSIM COR, and other relevant Government personnel.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 01**) for review and approval by the FEDSIM COR and the USSOUTHCOM TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (e.g., roles and responsibilities and lines of communication between contractor and Government).
c. Project Staffing Plan and status.
d. Draft Transition-In Plan (**Section F, Deliverable 10**) and discussion.
e. Security discussion and requirements (e.g., building access, badges, security clearances, Common Access Cards (CACs)).
f. Invoicing requirements.
g. Baseline Quality Management Plan (QMP) (**Section F, Deliverable 09**).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall provide a Kick-Off Meeting Minutes Report (**Section F, Deliverable 03**) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 1.3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J, Attachment E) (**Section F, Deliverable 04**). The MSR shall include at a minimum the following:

a. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (e.g., security clearance).
d. Government actions required.
e. Schedule (show major activities organized by Task/Subtask, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken and conferences attended (attach Trip Reports to the MSR for reporting period).
g. Costs incurred at the CLIN and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s), through the previous month.
h. Costs invoiced at the CLIN and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s), through the previous month.
i. Projected costs to be incurred at the CLIN and project level, broken out by prime contractor, subcontractor(s), and teaming partner(s), for the current month.

C.5.1.4 SUBTASK 1.4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting (**Section F, Deliverable 05**) with the USSOUTHCOM TPOC, FEDSIM COR, and USSOUTHCOM Government Representatives and Stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including

attendance, issues and risks discussed, decisions made, and action items assigned, to the FEDSIM COR (**Section F, Deliverable 06**).

C.5.1.5 SUBTASK 1.5 – PREPARE AND UPDATE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall document all requirements in a PMP (**Section F, Deliverable 07**) and shall provide it to the COR and TPOC.

The PMP shall provide, at a minimum:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
g. Include the contractor's QMP.

The PMP is an evolutionary document that shall be updated annually at a minimum and as program changes occur. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (**Section F, Deliverable 08**) when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment F.

C.5.1.7 SUBTASK 1.7 – PROVIDE QUALITY MANAGEMENT PLAN

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a QMP (**Section F, Deliverable 09**) and maintain and update it as changes in the program processes are identified. The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

C.5.1.8 SUBTASK 1.8 – PERFORMANCE SCORECARD

The contractor shall engineer, develop, deploy, maintain, and enhance the SCITES Scorecard Application (SSCA) (**Section F, Deliverable 19**) located on a Non-Secure Internet Protocol

Router Network (NIPRNet). The SSCA is used to collect task area performance results for the USSOUTHCOM SCITES program. The data gathered in the scorecards will be compiled to populate a series of dashboards at the task area, division, and program levels on a monthly basis. The SCCA shall be used by contractor program management, Task Area Leads and Task Managers, and Government Performance Monitors.

The SCCA shall include, but not be limited to, the following capabilities:

a. A training section offering access to new users to learn about the application and how to report and evaluate performance.
b. Individual scorecards for each task that include summaries of metrics, supporting documents, areas for Task Area Leads, Task Managers and Government Performance Monitors to provide input on contractor accomplishments and/or areas for improvement, as well as a subjective evaluation section for scoring.
c. An archived section offering access to the previous months' scorecards.
d. Sections describing each metric used on the TO.
e. A settings section to allow for user or role changes and assignments of backups.
f. A Frequently Asked Questions (FAQ) and Help section.
g. Automated calculations and rollups to populate the dashboard pages in real-time.
h. Automated notifications and workflows connected to the enterprise electronic mail (email) system.

C.5.2 TASK 2 – TRANSITION SERVICES

The contractor transition services shall include having all tasks staffed with fully qualified personnel, having a plan to integrate staff and ensure staff is fully trained, and taking over services with minimal to no degradation of services. The contractor shall assume full responsibility for management of all TO requirements, as well as have a plan to transition and deliver all material and information to the Government at the end of the TO.

C.5.2.1 SUBTASK 2.1 – TRANSITION-IN

The contractor shall provide a Transition-In Plan (**Section F, Deliverable 10**) as required in Section F. This Transition-In Plan shall include details on how the contractor will support the current legacy IT systems and related communications systems that are in place through the Transition-In period. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition-in. A comprehensive plan for establishing the NOSC, with start dates to be within the Transition-In period, shall be included in the Transition-In Plan.

In the Transition-In Plan, the contractor shall identify how it will coordinate with the outgoing contractor and/or Government personnel to transfer knowledge including, but not limited to, the following:

a. Program management processes.
b. POCs.
c. Location of technical and program management documentation.
d. Status of ongoing technical initiatives.

e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Inventory and Transfer of GFI/GFE from outgoing contractor to incoming contractor.
h. Schedules and milestones.
i. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-in.

The contractor shall implement its Transition-In Plan No Later Than (NLT) 10 calendar days after award, and all transition-in activities shall be completed NLT 90 calendar days after approval of the Transition-In Plan.

C.5.2.2 SUBTASK 2.2 – TRANSITION-OUT

The contractor shall provide transition-out services when required by the Government. The contractor shall provide a Transition-Out Plan (**Section F, Deliverable 11**) within six months of Program Start (PS). The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall review and update the Transition-Out Plan in accordance with the specifications in Sections E and F.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Program management processes.
b. POCs.
c. Location of technical and program management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.3 TASK 3 – OPERATIONS SERVICES

The contractor shall provide IT O&M of enterprise network operations; enterprise data center operations; vendor/provider agnostic on-premise, hybrid, and cloud-based IT operations; edge computing capabilities; data analytics operations; voice and video operations (e.g., Internet Protocol (IP) telephony, Video Teleconferencing (VTC), Public Switched Telephony Network (PSTN), Defense Red Switch Network (DRSN)), COOP/DR, and related training. In order to standardize all USSOUTHCOM IT management, processes, and services, USSOUTHCOM

seeks to redesign (over time) its current Service Management configuration and employ the DoD Enterprise Service Management Framework (DESMF) (as referenced in DoD Instruction (DoDI) 84401.01 and USSOUTHCOM and U.S. Army Network Enterprise Center (USANEC) policies). The contractor shall employ appropriate DESMF principals to reduce risk and cost while providing continuous service improvement to USSOUTHCOM IT customers.

C.5.3.1 SUBTASK 3.1 – ENTERPRISE NETWORK OPERATIONS SERVICES

The contractor shall provide enterprise network operations services to include, but not limited to, the following:

a. **OEM** – Network field service engineers shall be available at the Tier 4 level as required to service the current and future network environment. The contractor shall provide a Tier 3 IT problem solving solution and have the ability to identify, document, and resolve major problems. In addition, the contractor shall provide root cause analysis and training to reduce the use of Tier 4 escalation.

b. **Network Infrastructure O&M** – Irrespective of the network protocol (e.g., IPv4 or IPv6), and the classification of the network (e.g., Unclassified (UNCLASS), Secret, Top Secret (TS) and/or Sensitive Compartmented Information (SCI)) the contractor shall operate, monitor, alert, manage, maintain, install, and troubleshoot USSOUTHCOM network infrastructure devices and services (e.g., Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN)) . The contractor shall provide services for all aspects of network management and operations, including policies, procedures, implementation, technology integration, and guidance for both scheduled and unscheduled maintenance. The contractor shall manage the AO Uniform environment IP address plan. The contractor shall act as the USSOUTHCOM Public Internet Access Network (SPIAN), Joint Worldwide Intelligence Communications System (JWICS), Secret Internet Protocol Router Network (SIPRNet), NIPRNet, and any other AO Uniform network technical POC for the southcom.mil and southcom.smil.mil domains, as well as other domains that may be implemented throughout the course of performance of this TO.

c. **Network Security Hardware O&M** – Services shall include configuring, maintaining, analyzing, and monitoring data output from all network security hardware, including, but not limited to, the Security Information Event Management (SIEM) tool, in order to accurately detect and respond to threats across the AO Uniform environment. This includes services required to centralize all endpoint protection tools of the (e.g., Host-Based Security System/Endpoint Security Solution (HBSS/ESS)) NIPR/SIPR/SPIAN/JWICS administrative and management application functions for the AOR to the USSOUTHCOM NOSC.

d. **Secure Enclave Extension Capabilities** – The contractor shall provide all services required to manage, operate, and maintain the secure and non-secure Virtual Private Network (VPN) and Dynamic Multipoint Virtual Private Network (DMVPN) access and gateways on SIPRNet, NIPRNet, and SPIAN networks as well as any other AO Uniform network.

e. **Boundary Device O&M** – The contractor shall provide all services required to implement and maintain exterior DODIN connectivity as well as public internet

connectivity. This includes, but is not limited to, engineering, installation, and O&M of routers, switches, encryption devices, and ancillary equipment.

f. **Stand-Alone Networks** – Services required to provide stand-alone networks shall include, but are not limited to, engineering, installation, patching, maintenance, operations, and user services for these non-interconnected networks throughout the enterprise.

g. **Domain Name Service (DNS)** – The contractor shall provide internal and external IPv4 and IPv6 primary and secondary DNS services for USSOUTHCOM enterprise networks. The contractor shall make recommendations to configure and name DNS sub-domains. The contractor shall assist the Government in coordinating with Defense Information Systems Agency (DISA) and other organizations, where applicable, for DNS services.

h. **Monitoring and Management Solutions** – The contractor shall leverage the Fault, Configuration, Accounting/Administration, Performance, and Security (FCAPS) framework for network management. The contractor shall monitor, alert, and forecast problems before they arise, which is a key component to healthy and self-healing IPv4 and IPv6 networks. The contractor shall alert and consult the Government on any fault, performance, and/or security issues that may arise.

i. **Access Control** – The contractor shall operate and maintain enterprise applications and devices for network Authentication, Authorization, and Accounting (AAA), port authentication, network end-device compliance, device profiling, and policy compliance.

j. **Log Management** – The contractor shall configure and maintain all network equipment for log collection and retention according to applicable policies and regulations. This includes services to configure, maintain, analyze, and monitor data input and output from the SIEM tools in order to accurately detect and respond to problems, outages, and security threats across the AO Uniform, and provide intelligent insights that enable quick response measures to reduce the impact of incidents and proactively prevent future incidents. The contractor shall configure, test, fine-tune, and maintain all rule sets within SIEM, and ensure rule sets exhibit fluidity to adapt to changes within the AO Uniform environment. The contractor shall analyze and investigate all alerts/offences generated within SIEM on a daily basis, and resolve offences upon termination of analysis/investigation. The contractor shall analyze and fine-tune rule sets to reduce false positives within the SIEM.

k. **IP Address Management (IPAM)** – The contractor shall manage the IPAM plan in an automated system. The contractor shall act as the NOSC's technical POC for all USSOUTHCOM AO Uniform networks, as well as for the southcom.mil and southcom.smil.mil domains. The contractor shall coordinate with network managers of the SIPRNet and NIPRNet as well as other AO Uniform networks to maintain and update the DoD Network Information Center (NIC) website on all domain or IP issues (as of the original issuing of the TO, the NIC website Uniform Resource Locator (URL) is: https://nic.mil/). The contractor shall maintain and update the Network Address Declaration (NAD) IP document.

l. **Dynamic Host Configuration Protocol (DHCP) Management** – The contractor shall operate and maintain the USSOUTHCOM DHCP services for all data- and voice-supported networks.

m. **Call Center/Service Desk Services** – The contractor shall provide 24 hours per day, seven days per week (24x7) service desk operations. The contractor shall provide call center/service desk services to both remote and walk-in customers throughout the USSOUTHCOM enterprise that have issues requiring resolution. These services include, but are not limited to, managing network accounts, password creation and resets, resetting Common Access Card (CAC) Personal Identification Numbers (PINs), issuing and tracking, and providing configuration and management of SIPRNet and NIPRNet Token Cards. Additionally, the contractor shall engineer, install, operate, and maintain a problem tracking solution that shall monitor and track the status of all submitted incidents, problems, and changes, including cases where they are escalated to higher level services. This system shall be capable of reporting and trend analysis reports. The contractor shall provide the services required for user account creation, management, and administration across multiple classified and unclassified environments including, but not limited to, DISA's Defense Enterprise Email (DEE), and Army Message Handling System (AMHS). The contractor shall develop, deploy, and maintain a customer-facing self-help knowledge repository for problem resolution. During normal duty hours, the contractor shall provide incident problem identification and response times within 15 minutes for the USSOUTHCOM enterprise.

C.5.3.2 SUBTASK 3.2 – ENTERPRISE DATA CENTER OPERATIONS SERVICES

The contractor shall provide enterprise data center operations services that include, but are not limited to, the following:

a. **OEM Data Center Field Engineer Services** – OEM data center Field Engineer services at Tier 4 level are required for the current and future data center environment. The contractor's Field Engineers shall provide Tier 3 staff with IT problem solving. The Field Engineers shall have the ability to identify, document, and resolve major problems. In addition, the Field Engineers shall provide root cause analysis and training to reduce the use of Tier 4 escalation.

b. **O&M**

1. **Storage** – The contractor shall manage, update, and troubleshoot all Storage Area Network (SAN) and other storage technology devices across the USSOUTHCOM enterprise.
2. **Backups** – USSOUTHCOM requires backup services including file-level and system-level recovery services. The contractor shall develop and implement a successful Backup Plan (**Section F, Deliverable 12**) that supports both the traditional IT backup architecture as well as the DR and COOP plans of USSOUTHCOM. The Backup Testing Schedule (**Section F, Deliverable 13)** of the Backup Plan shall be completed according to the schedule, and Backup Testing Results (**Section F, Deliverable 14**) shall be published in accordance with. DR and COOP Exercise Testing Results (**Section F, Deliverable 15)** shall be documented in coordination with USSOUTHCOM DR and COOP exercises as directed by USSOUTHCOM.
3. **Virtualization** – The contractor shall provide virtualization services of physical systems (P2V) and the reverse (V2P) if needed. Additionally, the contractor shall provide services for virtualized platforms and systems which include, but are not limited to, automated system provisioning, deployment, and servicing of multiple

physical and virtual enclaves. These enclaves can be local or cloud based (hybrid, on premise, and off premise) and could be private, Government cloud provider, or public cloud provider hosted.

4. **Operating Systems** – USSOUTHCOM requires full systems services for multiple operating systems including, but not limited to, Linux and common derivatives thereof (e.g., RedHat, Apache) as well as multiple versions of Microsoft Windows (server and client operating systems).
5. **Print and Scan Services** – The contractor shall provide enterprise print, scan, and fax capabilities through multiple office automation platforms. The contractor shall provide full remote management systems engineering, installation, and O&M for all office automation platforms.

c. **Active Directory (AD)** – The contractor shall provide all AD management services including, but not limited to, Public Key Infrastructure (PKI), DNS, DHCP, group policy, certificates, and Active Directory Federation Services (ADFS).

d. **Application Operations** – USSOUTHCOM requires services covering engineering, installation, and O&M of various applications and their operating environments. This includes, but is not limited to, collaboration portals (e.g., SharePoint), messaging platforms (e.g., Skype), custom applications, Office productivity (e.g., Microsoft Office), Concurrently Located (CO-LO) systems and networks, hosted systems, and database systems (e.g., Structured Query Language (SQL), Oracle), the Joint Detainee Information Management System (JDIMS), Detainee Information Management System, and any replacement systems.

e. **Systems Operations** – The contractor shall provide systems operations services including manual and automated processes to perform activities such as imaging, patching, application deployment, system monitoring, application monitoring, and VDI service operations.

f. **End User Device Operations** – USSOUTHCOM requires engineering, installation, and O&M services for multiple end-user device types. These services include, but are not limited to, manual and automated provisioning/de-provisioning, thin/zero client services, imaging, monitoring, patching, and application virtualization.

g. **Password Management Suite** – The contractor shall engineer, install, operate, and maintain a password management suite that shall be available to all enterprise users on a roles and individual-based permissions system, implemented on each of USSOUTHCOM's AO Uniform networks.

h. **Log Management** – The contractor shall configure and maintain all systems devices for log collection and retention according to applicable policies and regulations. This includes services to configure, maintain, analyze, and monitor data input and output from the SIEM tools. The contractor shall accurately detect and respond to problems, outages, and security threats across the AO Uniform environment, and provide intelligent insights that enable quick response measures to reduce the impact of incidents and proactively prevent future incidents. The contractor shall configure, test, fine-tune, and maintain all rule sets within SIEM, and ensure rule sets exhibit fluidity to adapt to changes within the AO Uniform environment. The contractor shall analyze and investigate all alerts/offences generated within SIEM on a daily basis and resolve offences upon termination of analysis/investigation. The contractor shall analyze and fine-tune rule sets to reduce false positives within the SIEM.

C.5.3.3 SUBTASK 3.3 – VOICE AND VIDEO OPERATIONS SERVICES

The contractor shall provide voice and video operations services including, but not limited to, the following:

a. **Public Address (PA) and Live Audio Reinforcement** – The contractor shall provide PA system services for all functions, ceremonies, and media events (approximately 15 to 30 events per year). These services include O&M during events, setting up and tearing down systems and equipment, and pre-event functionality testing to ensure that all PA systems and associated equipment are 100 percent operational and capable of meeting event requirements.
b. **Internet Protocol Television (IPTV)** – The contractor shall provide engineering, installation, and O&M of USSOUTHCOM IPTV networks. This includes enterprise-wide multicast distribution, head-end facilities incorporating up to approximately 75 streams concurrently, and digital archiving of special events.
c. **Community Access Television (CATV)** – The contractor shall coordinate with local commercial service providers to integrate and rebroadcast commercially available television channels. This includes channel package selection; installation, engineering, and O&M of client-side equipment; and outage resolution.
d. **Digital Signage** – The contractor shall provide services for engineering, installation, and O&M of digital signage presence points throughout the AOR for command information distribution.
e. **DRSN** – The contractor shall provide services for DRSN Switchboard Operators. This includes, but is not limited to, Joint Operations Center (JOC) DRSN services, conference call facilitation, directory assistance, and direct dial assistance. Additionally, USSOUTHCOM requires engineering, installation, and O&M of DRSN nodes. This includes, but is not limited to, DRSN red and black switches, interconnection equipment, end-user device terminals, interconnectivity with radio operations, encryptions equipment, and long-haul circuit facilitation.
f. **PSTN** – The contractor shall provide services for the PSTN, including all connectivity and end-user equipment engineering, installation, and O&M. Additionally, services for emergency trunk transfer lines and interconnecting circuits are required. The contractor shall coordinate with commercial, Government, foreign government, and DoD service providers for outage resolution, service installation, and termination.
g. **Plain Old Telephone System (POTS)/Analog Voice** – The contractor shall provide services to multiple analog voice and POTS telephony devices. This includes engineering, installation, and O&M of phone switches, end-user devices, voicemail services, interconnectivity, and interoperability of all devices.
h. **Digital Voice** – The contractor shall provide services to digital voice technologies, including, but not limited to, Voice over Internet Protocol (VoIP), Secure Voice over Internet Protocol (SVoIP), Voice over Secure Internet Protocol (VoSIP), Enterprise Classified Voice over Internet Protocol (ECVoIP) devices, and wireline encryption devices (e.g., Sectéra/Viper/STE).
i. **Visual Information Systems (VIS)** – The contractor shall engineer, install, operate, and maintain the USSOUTHCOM VIS. This includes, but is not limited to, VTC devices,

teleconferencing services, Audio-Visual (A/V) services, desktop collaboration services, and multi-display clocks for the entire USSOUTHCOM AO.

1. **Scheduling/Facilitation** – The contractor shall schedule, coordinate, and administer multiple simultaneous conferences, VTC sessions, A/V events, and press conferences to include events that may require contractor presence after hours and/or on the weekend.
2. **Direct On-Site Services of VTC** – The contractor shall provide on-site, in-room services for Very Important Person (VIP) VTC conferences, including providing O&M and troubleshooting services in real-time during Government-identified events.
3. **Remote Services** – The contractor shall provide remote services including telephonic troubleshooting and remote system login for troubleshooting, configurations, and O&M.
4. **A/V System Automation** – The contractor shall provide engineering, installation, and O&M of A/V system automation systems including, but not limited to, code development, Graphical User Interface (GUI) development, Codec integration, video switchers, and audio switchers over multiple platforms (e.g., Extron, Crestron, AMX, and others).

j. **Video Wall** – The contractor shall provide engineering, installation, and O&M of video wall systems. This includes, but is not limited to, color balance, contrast, and alignment; technology research for emergent trends that can meet the needs of new requirements; and brightness adjustments.

k. **OEM VTC Field Engineer Services at Tier 4 Level** – The contractor shall provide current and future VTC and collaboration environment services. The Field Engineers shall provide Tier 3 staff with IT problem solving. The contractor shall have the ability to identify, document, and resolve major problems. In addition, the contractor shall provide root cause analysis and training to reduce the use of Tier 4 escalation.

l. **Hours of Operation -** The contractor shall provide Conference Room Support Services typically from 0600-1900 Monday-Friday local time at USSOUTHCOM HQ, JTF-Bravo, JTF-Guantanamo (GTMO), and Bogota, Colombia. The contractor shall also be prepared to extend these service hours to include evenings and weekends when required by the Government (e.g., real-world missions, contingencies and exercises, and other customer requirements).

C.5.3.4 SUBTASK 3.4 – CYBERSPACE OPERATIONS (CO) EXERCISE SERVICES

The contractor shall provide exercise services to include planning, execution, and assessment of CO for all USSOUTHCOM exercises. The contractor shall assist in building realistic, challenging, and relevant cyberspace exercise scenarios that meet the following strategic and operational exercise objectives for USSOUTHCOM. The contractor shall provide CO exercise services including, but not limited to, the following:

a. End-to-end cyberspace exercise services including scheduling, coordinating, and conducting planning meetings, work group meetings, and exercise facilitation.

b. Represent the organization as the prime technical cyberspace exercise POC during exercise planning, execution, and post exercise. Interact with senior external personnel on significant technical matters often requiring coordination between organizations.

c. Input to briefings and transitioning concepts to execution and assist in the coordination of joint operational planning in support of training, combat, and contingency operations.
d. Input for the development of cyberspace Tactics, Techniques and Procedures (TTPs), Concept of Operations (CONOPS), Courses Of Action (COAs), and other related documents.
e. Input to address shortfalls, prioritize and validate requirements, and be prepared to modify development planning efforts based on the changing cyberspace environment.
f. Gather and analyze facts, draw conclusions, conduct analysis, devise recommended solutions, and package the entire process into briefings, papers, or reports suitable for executive-level leadership in accordance with Cyberspace Operations Exercise Results (**Section F, Deliverable 20**).

C.5.3.5 SUBTASK 3.5 – CONTINUITY OF OPERATIONS (COOP) AND DISASTER RECOVERY (DR) SERVICES

The contractor shall design, transition, and operate a COOP for the entire USSOUTHCOM enterprise, including the three enduring JTFs and all SCOs. The COOP shall include emergency, contingency, and/or recovery operations.

The contractor shall accomplish failover testing to internal backup systems and to external replication sites. To meet the failover testing requirement, the contractor shall prepare and maintain COOP and DR operations artifacts including, but not limited to, documentation, test results, plans, Command Cyber Readiness Inspections (CCRI), and Contributing Factors in accordance with DR and COOP Exercise Testing Results (**Section F, Deliverable 15**).

C.5.3.6 SUBTASK 3.6 – TRAINING SERVICES

The contractor shall develop and provide training services and Training Documentation (**Section F, Deliverable 21**) for all COTS, GOTS, and custom-developed software created, procured, or maintained through this TO including, but not limited to, hard-copy written manuals, soft-copy written manuals, training aids, classroom-based training, computer-based training, one-on-one live training, and train the trainer. The contractor shall provide current training performed for JDIMS and DIMS.

C.5.3.7 SUBTASK 3.7 COMMAND AND CONTROL INTEROPERABILITY BOARD (CCIB) SERVICES

The contractor shall provide CCIB services in three categories – Event Liaison Services, Travel, and Scheduling. The location of the scheduled CCIB events include, but are not limited to, the Partner Nation country, USSOUTHCOM HQs, any USSOUTHCOM component HQs, and the National Capital Region (NCR). Travel to the CCIB location is expected. The contractor shall provide the following CCIB services:

a. CCIB Event Liaison Services:
    1. Coordinate event budget planning and expenditure tracking and reporting activities for CCIB events.
    2. Coordinate on-site services for CCIB events, including catering, facilities, and supplies.
    3. Coordinate with the Joint Engagement Visitors Bureau (JEVB).

4. Coordinate attendee registration.

b. CCIB Travel:
   1. Coordinate official passport, visa, Aircraft and Personnel Automated Clearance System (APACS), and Joint Personnel Adjudication System (JPAS) clearance verification requests.
   2. Coordinate travel prerequisite training requirements.
   3. Act as primary the Defense Travel System (DTS) representative for CCIB for coordination of travel, lodging, and transportation.

c. CCIB Scheduling:
   1. Create and manage comprehensive CCIB schedules unique to each CCIB event.
   2. Create and manage a consolidated repository of discussion points and topics into a CCIB Summary Report (**Section F, Deliverable 29**).
   3. Create and manage the consolidated CCIB Action Item Tracking Report (**Section F, Deliverable 30**), providing updates to CCIB at routine intervals between CCIB events.

C.5.4 TASK 4 – TRANSPORT SERVICES

The contractor shall provide IT transport services, including Tech Control Facility (TCF) and Patch and Test (P&T). The contractor shall provide transport services including, but not limited to, handling of long-haul circuit-type operations, Satellite Communication (SATCOM), inside plant cabling, outside plant cabling, node site coordinator handling of Department of State (DoS) liaison services, as well as remote site installs and data center infrastructure services. The contractor should also be prepared to extend its service hours to include evenings and weekends when required by the Government (e.g., real-world mission, contingencies and exercises, and other customer requirements).

C.5.4.1 SUBTASK 4.1 – TECH CONTROL FACILITY (TCF) AND PATCH AND TEST (P&T) SERVICES

The contractor shall provide TCF and P&T services for engineering, installation, and O&M. The equipment the contractor shall provide TCF and P&T services for includes, but is not limited to:

a. Matrix switches
b. Multiplexors
c. Demultiplexors
d. Inverse multiplexors
e. Fiber optic modems
f. Channel service units
g. Data service units
h. Various encryption and decryption devices at TCF and P&T facilities across the enterprise

The contractor shall provide the installation, maintenance, and termination of long-haul communications circuits carrying vital mission telecommunications traffic. These circuits and equipment shall be operated and maintained on various transmission mediums including, but not limited to, copper, fiber optic, breach/free space optics, satellite, and terrestrial Radio Frequency

(RF) (e.g., microwave, High Frequency (HF), Ultra High Frequency (UHF), and Very High Frequency (VHF)). This includes circuit actions functions of both DoD and commercial lease circuits as well as others. In coordination with multiple USG agencies such as DISA and Defense Information Technology Contracting Organization (DITCO), as well as host nation Government agencies, the contractor shall perform engineering, connection, disconnection, and O&M for all AO Uniform network circuit connection points and points of demarcation at the direction and approval of USSOUTHCOM.

C.5.4.2 SUBTASK 4.2 – LAND MOBILE RADIO (LMR)

The contractor shall provide services to engineer, install, operate, and maintain LMR networks and their ancillary equipment. This includes, but is not limited to, frequency management actions, base station radios, vehicle-mounted radios, handheld radios, man-packable radios, and various antenna platforms (e.g., mobile, base station, and portable).

C.5.4.3 SUBTASK 4.3 – SATELLITE COMMUNICATION (SATCOM)

The contractor shall provide SATCOM services to the USSOUTHCOM SATCOM architecture, including, but not limited to, services for Very Small Aperture Terminal (VSAT), Military Strategic and Tactical Relay (MILSTAR), and Broadband Global Area Network (BGAN). This shall include node site coordination with both DoD and commercial service providers, frequency management and de-confliction, bandwidth planning, contingency operations, and capabilities planning and management.

C.5.4.4 SUBTASK 4.4 – CABLE PLANT SERVICES

The contractor shall provide cable plant services including, but not limited to, inside and outside cable plant, throughout the enterprise. Cable plant services include, but are not limited to, fiber and copper cabling, low voltage cabling, direct burial cabling, aerial cabling, conduit, innerducting, main distribution frame, intermediate distribution frame, patch facility, data center, facility, and end-user services.

C.5.4.5 SUBTASK 4.5 – WIRELESS NETWORK INFRASTRUCTURE SERVICES

The contractor shall engineer, install, operate, and maintain all wireless network infrastructure including, but not limited to, all access points, controllers, access control, and security devices.

C.5.4.6 SUBTASK 4.6 – NODE SITE COORDINATOR

The contractor shall provide node site coordinator services that include, but are not limited to, coordination with U.S. Government agencies, DoD (e.g., DISA and DITCO), DoS, host-nation Government agencies, and commercial service providers at the direction and approval of USSOUTHCOM. These coordination activities are in support of circuit actions for remote site installs, local inside and outside plant cabling permits and authorizations, site surveys, and other activities.

C.5.5 TASK 5 – AO UNIFORM CONSTRUCTED NETWORK OPERATIONS AND SECURITY CENTER (NOSC) SERVICES

The contractor shall provide enterprise NOSC services, to include network monitoring and management; Tier 3 CSSP activities and management, analysis, infrastructure support, incident response and auditing; JRSS O&M, and SIEM O&M.

C.5.5.1 SUBTASK 5.1 – AO UNIFORM CONSTRUCTED NETWORK SECURITY ASSESSMENT SERVICES

The contractor shall provide engineering, installation, and O&M services to provide both situational awareness and threat and vulnerability assessment across the enterprise. The contractor shall utilize a combination of services, including, but not limited to, endpoint security solutions, scanning tools (e.g., HBSS, Assured Compliance Assessment Solution (ACAS), and Security Content Automation Protocol (SCAP)), threat analysis solutions, compliance-level evaluation tools, and vulnerability assessment systems.

C.5.5.2 SUBTASK 5.2 – AO UNIFORM CONSTRUCTED NETWORK COMMON OPERATIONAL PICTURE (NETCOP) SERVICES

The contractor shall provide engineering, installation, and O&M services to provide NETCOP status awareness of Layers 1 through 7 of the Open Systems Interconnection (OSI) model for USSOUTHCOM AO Uniform constructed networks. This includes, but is not limited to, graphical representation of the status of all enterprise interconnectivity and assets such as routers, switches, endpoint devices, storage systems, systems of systems, compute platforms, and servers, both physical and virtual. The NETCOP solution shall provide analytical capabilities to facilitate fault detection and root cause failure analysis through interconnectivity with other enterprise monitoring and logging solutions.

The contractor shall also identify, determine/verify the operational impacts (in coordination with the affected organization), and report on all outages and degradations of data/voice/video services/applications throughout the enterprise. The contractor shall provide a near real-time status of IT services and Authorized Service Interruptions (ASIs) via Government-required notifications, a dashboard, and regular briefings with the Government as directed. The contractor shall directly contact and brief USSOUTHCOM leadership on major NETOPS events and appropriate on-call staff for after–duty-hours events in accordance with established SOPs. The contractor shall track these NETOPS events in a tailored tracking database and/or ticket tracking system. The contractor shall review, verify, coordinate, and de-conflict all ASI requests from agency partners, direct reporting units, component commands, JTFs, and internal USSOUTHCOM organizations. The contractor shall directly update USSOUTHCOM leadership on major ASI events in accordance with established SOPs. The contractor shall track these ASI events in a tailored tracking database and/or ticket tracking system. The contractor shall perform personal accountability (on demand) tracking and reporting in accordance with SOPs and shall monitor and maintain Organizational Message System (OMS) and Automated Message Handling System (AMHS) feeds.

C.5.5.3 SUBTASK 5.3 – AO UNIFORM CONSTRUCTED NETWORK TIER 3 CYBERSECURITY SERVICE PROVIDER (CSSP) SERVICES

The contractor shall provide engineering, installation, and O&M of a Tier 3 CSSP system of systems and infrastructure. The contractor shall provide services for monitoring, management, analysis, auditing (e.g., vulnerability reports, scorecards, Security Technical Implementation Guides (STIGs), and CTOs), forensics, and incident response. These roles and responsibilities are doctrinally founded in DISA's CSSP program as directed by the Joint Chiefs of Staff's Joint Publication 3-12 "Cyberspace Operations."

C.5.5.4 SUBTASK 5.4 – AO UNIFORM CONSTRUCTED NETWORK OPERATIONS AND SECURITY CENTER (NOSC) ORIGINAL EQUIPMENT MANUFACTURER (OEM) SERVICES

The contractor shall provide field engineer services for NOSC-specific systems at the Tier 4 level for the current and future NOSC environment. Field engineering services include, but are not limited to, providing Tier 3 staff with IT problem solving; the ability to identify, document, and resolve major problems; and root cause analysis and training to reduce the use of Tier 4 escalation.

C.5.5.5 SUBTASK 5.5 – SECURITY COOPERATION TAILORED TRAINING EVENTS SERVICES

The contractor shall provide tailored cyber security training and Training Documentation (**Section F, Deliverable 21**) with partner nations in the USSOUTHCOM AOR. The offeror shall provide in-person training sessions approximately twice a year for approximately four countries in the AOR (approximately eight training sessions in total). All events shall be in coordination with the cognizant USG agency to ensure International Traffic in Arms Regulations (ITAR) compliance for defense-related articles and services on the United States Munitions List (USML). At a minimum, the tailored trainings shall include:

a. Training in the partner nation's native language.
b. Tailored vendor-specific training for the relevant cyber security tools, so that, at a minimum, the partner nation's cyber security operators can:
    1. Operate their own commodity cyber security tools to provide effective cyber defense to their respective countries.
    2. Determine threats on their networks and share the threat information with USSOUTHCOM, leveraging an enduring Mission Partner Environment (MPE) network, and other technical means in near real-time.
    3. Receive indications of threat that USSOUTHCOM shares with them and have the technical knowledge to dynamically posture their cyber security tools to alert against the particular threat and report findings back to USSOUTHCOM.

C.5.5.6 SUBTASK 5.6 – AO UNIFORM CONSTRUCTED NETWORK SECURITY DEVICES SERVICES

The contractor shall provide services to multiple enterprise security devices (physical and virtual) including, but not limited to, firewalls, intrusion detection devices, intrusion protection devices, endpoint protection devices, wireless security systems, and insider threat protection

systems. The contractor shall, at a minimum, provide analysis of threats, response to threats, rules creation, security level evaluation, and penetration vulnerability assessments.

C.5.5.7 SUBTASK 5.7 – AO UNIFORM CONSTRUCTED NETWORK SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SERVICES

The contractor shall provide AO Uniform enterprise-wide engineering, installation, and O&M of a holistic SIEM solution to perform analysis and reporting on data collected by the log management solutions implemented throughout the enterprise. These enterprise-level SIEM solutions shall accurately detect and respond to problems, outages, and security threats across the AO Uniform environment and provide intelligent insights that enable quick response measures to reduce the impact of incidents. The contractor shall configure, test, fine-tune, and maintain all rule sets within SIEM, and ensure rule sets exhibit fluidity to adapt to changes within the AO Uniform environment. The contractor shall analyze and investigate all alerts/offenses generated within SIEM on a daily basis and resolve offences upon termination of the analysis/investigation. The contractor shall analyze and fine-tune rule sets to reduce false positives within the SIEM and produce proactive approaches to prevent future vulnerabilities.

C.5.5.8 SUBTASK 5.8 – AO UNIFORM CONSTRUCTED NETWORK CYBER ANALYTICS-AS-A-SERVICE

The contractor shall provide USSOUTHCOM with cyber analytics-as-a-service across the Theater (HQ and Direct Reporting Units (DRUs)). Currently, this service is partially available on the NIPRNet enclave of USSOUTHCOM's networks. The service will expand to other constructed networks within USSOUTHCOM, including the SIPRNet. Data sources will include additional sources of telemetry, to include User Activity Monitoring (UAM) tools. All analytics information is consumed within the USANEC-S NOSC and is to be projected to the USSOUTHCOM Joint Cyber Center (JCC) and analyzed by both the J3 JCC and USANEC-S NOSC.

The primary objective is to provide effective situational awareness of the cyber domain and defense techniques with a broader view of actor activity, motives, and attribution. This shall involve combining traditional cyber data sources such as attack and malware signatures, threat actor IP address, and malicious domains, with more advanced sources including unsupervised learning, memory analytics, system integrity validation metrics, and automated malware decomposition and analysis. This service shall be intuitive, allowing the operator/analyst to customize the visualization capabilities and provide relevant, operationalized data to USSOUTHCOM decision makers so they can take appropriate action to defend their enterprise and continue operations in a contested domain. The integration of cyber-related indicators, threat information, and transactional data facilitates the discovery of the "unknown - unknowns." These diverse, trusted data sources improve the overall service capability. These data sources build an image of how threat actors move across various global infrastructures. A traditional major barrier has been the speed at which analytics can be applied along with the ability to fuse disparate and unstructured data. The solution and services provided shall address these issues and include, but not be limited to, the following features:

a. Real-time, up-to-date information regarding sophisticated threat actors (threat actor profiles).
b. Cyber data acquisition and subject matter expertise capabilities.

c. An automated analytics capability to identify and assess malicious software artifacts at high-volume scales that is also capable of identifying false positives and negatives and flagging them for human review.
d. Computing hardware memory collection for analysis capability.
e. Threat actor and malicious activity mapping in virtual space.
f. Geolocation and subsequent graphical map display of a live, up–to-date fused dataset of the genuine geolocation of identified activities.
g. Monitoring of operational, real-time data sources (e.g., Publicly Available Information (PAI), Commercially Available Information (CAI), DoD information, and Other Government Agency (OGA) information).
h. Visualization capabilities to create interactive, operationalized role-based dashboards, reports, and dynamic alarming in real time.
i. Community detection which shall provide analytic evaluation and reporting of the community with which known bad actors associate.
j. Events/cases shall be correlated to cyber kill-chain elements in an automated fashion.

All applicable results and analysis shall be integrated into the USSOUTHCOM Battle Rhythm. Surge support of analytic expertise shall be provided during exercises and contingencies.

C.5.6 TASK 6 – COMPLIANCE AND PERSONNEL SECURITY SERVICES

The contractor shall provide compliance and personnel security services to include Communications Security (COMSEC), COMSEC Controlled Items (CCI), personnel security, physical security, and Authorization and Accreditation (A&A) packages. The contractor shall also be prepared to extend its service hours to include evenings and weekends when required by the Government (e.g., real-world missions, contingencies and exercises, and other customer requirements).

C.5.6.1 SUBTASK 6.1 – COMSEC SERVICES

The contractor shall provide COMSEC services that include, but are not limited to, COMSEC responsible officers, COMSEC account managers, COMSEC hand receipt holders, and COMSEC end users. These services also include acquisition, receipt, control, shipment, and destruction of COMSEC keying material, hardware, and software for USSOUTHCOM. The contractor shall prepare COMSEC documentation that includes, but is not limited to, destruction records, incident reporting, inventories, and compliance reports. The contractor shall monitor all COMSEC material handlers for regulatory compliance and report instances of noncompliance accordingly. The contractor shall provide services for CCI issues, turn-ins, tracking, shipping, disposal, and inventory.

C.5.6.2 SUBTASK 6.2 – PHYSICAL SECURITY

The contractor shall provide engineering, installation, and O&M services to safeguard all information, property, equipment, and materials. Documentation such as Standard Forms (SF) 700, 701, and 702, physical security logs, and visitor access logs shall be used to meet this requirement. Services shall include key control, GSA-approved storage device program management, combination management, and document control.

C.5.6.3 SUBTASK 6.3 – AUTHORIZATION AND ACCREDITATION (A&A) SERVICES

The contractor shall provide A&A services to create and maintain A&A packages for all enterprise devices, systems, networks, and systems of systems. The contractor shall develop, deploy, operate, and maintain approved solutions to monitor for A&A compliance. These packages and compliance evaluations shall be in support of applicable DoD and USG programs including, but not limited to, the Risk Management Framework (RMF) and Enterprise Mission Assurance Support Services (eMASS). The contractor shall provide assistance with regular reporting on compliance and A&A package tracking.

C.5.6.4 SUBTASK 6.4 – PERSONNEL SECURITY SERVICES

The contractor shall provide personnel security services to verify, create, validate, and/or maintain security clearance records on behalf of USSOUTHCOM in US Government systems of record such as the Joint Personnel Adjudications System (JPAS) and Secure Web Fingerprint Transmission (SWFT). The contractor shall create, distribute, and archive personnel security related documents including but not limited to deployment letters, visit requests, badging documentation, and administrative access letters.

C.5.7 TASK 7 – PROJECTS, INTEGRATION, AND ENGINEERING (PIE) SERVICES

The contractor shall provide IT project management services for IT projects throughout the enterprise. This includes all facets of project management in multiple methodologies including, but not limited to, the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK), Waterfall, Agile, hybrid, scrum, critical path method, critical chain project management, and integrated project management.

The contractor shall provide engineering services for new initiatives or new technologies to include OEM consultants. The contractor shall engineer and integrate all new solutions into the enterprise for the following areas: network, system, storage, data center, and facilities engineering. The contractor shall provide software development and systems integration for enterprise IT initiatives, delivering completed solutions for implementation into the USSOUTHCOM AO Uniform constructed networks. The contractor shall employ elements and principles of DevSecOps utilizing a tailored, consistent, and adhered-to DevSecOps model. USSOUTHCOM seeks to institutionalize this coordinated and consistent DevSecOps model with services that employ the best practices of mature, Agile-enabled organizations. Automated workflows that reduce manual process time and human interaction are needed to enable these solutions. The resultant DevSecOps model shall reduce technical debt and risk through increased security, increased efficiencies, reductions in the cost of O&M, and improved accuracy and timeliness in the delivery of functionality. These initiatives and new technologies shall be in support of the Enterprise Architecture plans as developed by the contractor and submitted to the Government for approval through the change management process. The contractor shall continuously evaluate the Enterprise Architecture plans and roadmaps and recommend improvements to USSOUTHCOM.

The contractor shall also be prepared to extend its service hours to include evenings and weekends when required by the Government (e.g., real-world missions, contingencies and exercises, and other customer requirements).

C.5.7.1 SUBTASK 7.1 – INFORMATION MANAGEMENT (IM)

The contractor shall develop, operate, maintain, manage, and integrate IM resources and activities for an enterprise-wide IM program for AO Uniform. The contractor shall develop and integrate tools to provide services to command and staff processes, activities, and tasks and shall provide training and awareness of IM resources throughout USSOUTHCOM enterprise. The contractor shall create, own, and execute IM, along with change adoption and communication plans, for all assigned changes being implemented. The contractor shall develop the Information Management Plan and Recommendations (**Section F, Deliverable 22**) on how to better utilize existing information systems and collaboration tools. The contractor shall provide and maintain USSOUTHCOM enterprise taxonomy and content management for all Secure Internet Protocol Router (SIPR) and Non-Secure Internet Protocol Router (NIPR) portal environments to include on and off premise. The contractor shall include recommendations on the management and design of USSOUTHCOM's enterprise portal site collections and sites to enhance an IM program. The contractor shall provide Innovation and Technology Plans and Recommendations (**Section F, Deliverable 23**) that further the mission and IM goals.

C.5.8 TASK 8 – LOGISTICS SERVICES

The contractor shall provide integrated logistics services, to include diplomatic pouch services, IT property management, mobile device management, purchase order planning and associated documentation, facilitation and coordination with Defense Reutilization Marketing Office (DRMO), asset management, Internet of Things (IoT), and lifecycle management. The contractor shall also be prepared to extend its service hours to include evenings and weekends when required by the Government (e.g., real-world missions, contingences and exercises, and other customer requirements).

C.5.8.1 SUBTASK 8.1 – WAREHOUSE SERVICES

The contractor shall develop, implement, and maintain a Warehouse Operations and Transportation Plan (**Section F, Deliverable 16**) to ship, receive, and store all IT equipment. Warehouse locations include, but are not limited to, USSOUTHCOM HQ, JTF-Bravo, and JTF-GTMO.

C.5.8.2 SUBTASK 8.2 – VEHICLE OPERATIONS SERVICES

The contractor shall provide Vehicle Operations Services in support of IT and ancillary equipment logistics throughout the AOR. These services include, but are not limited to, operations of tractor-trailer, straight truck, forklift, delivery van, passenger van, SUV and sedan. The vehicles will include a mixture of Government owned, government leased/rented, and contractor leased/rented under Government reimbursement.

The contractor shall develop and implement a vehicle safety program in accordance with applicable laws and regulations. All contractor vehicle operators shall be properly licensed for the equipment they are operating. Vehicles operated in the course of performing this TO include, but are not limited to, USG-owned, leased, and rented vehicles. Vehicle Operations Services include but are not limited to transporting IT equipment between USG warehouses and transporting contractor personnel throughout the AOR. Additionally, Government-approved and contractor-leased and/or rented vehicles (with Government reimbursement) under this TO shall be included in the Warehouse Operations and Transportation Plan.

If the contractor requires the lease of vehicles, it shall notify the USSOUTHCOM TPOC and FEDSIM COR to determine if Government-provided equipment is available. If Government vehicles are not available to support the mission, the contractor may lease vehicles for operation in accordance with Section H.20.1. The contractor shall submit justifications for lease of equipment and track any resulting leased equipment in a Commercial Leasing Report (Section F, Deliverable 28).

The Commercial Leasing Report shall include:

a. Date of lease.
b. Date material/equipment was received by the contractor.
c. Lease cost and any additional costs associated with the leased equipment throughout the lease period.
d. Frequency the material/equipment was used (e.g., miles, hours).
e. Date the material/equipment was returned and lease completed.

C.5.8.3 SUBTASK 8.3 – SHIPPING AND RECEIVING SERVICES

The contractor shall provide shipping and receiving including, but not limited to, packaging, preserving, and shipping the hardware, digital and associated materials required for IT systems to include COMSEC, in support of this TO. The contractor shall utilize diplomatic locations throughout the USSOUTHCOM AOR, as well as coordinate the shipping, receiving, and escorting of all shipments as necessary.

C.5.8.4 SUBTASK 8.4 – MOBILE DEVICE MANAGEMENT

The contractor shall provide services to receive, maintain accountability, and distribute classified and unclassified mobile devices and equipment including, but not limited to, pagers, voice-only devices, smartphones, and portable data devices. At a minimum, the contractor shall provide services for device provisioning, configuration, setup, local and remote management, and security services. The contractor shall develop a Mobile Device Report (**Section F, Deliverable 24**) that provides analysis and evaluation on accounts, billing, and usage statistics.

C.5.8.5 SUBTASK 8.5 – ASSET MANAGEMENT IN COORDINATION WITH DEFENSE REUTILIZATION MARKETING OFFICE (DRMO) SERVICES

The contractor shall provide services for turn in of assets to the DRMO. This includes, but is not limited to:

a. Create and maintain any requisite paperwork.
b. Coordinate with the FEDSIM COR, USSOUTHCOM TPOC, and Property Book Officer before turning in equipment or components.
c. Maintain a Defense Reutilization Marketing Office Log (**Section F, Deliverable 25**) of all equipment or components turned into DRMO.

C.5.8.6 SUBTASK 8.6 – CONFIGURATION MANAGEMENT (CM)

The contractor shall provide services for engineering, installation, and O&M of a CM system to include a CM Plan (**Section F, Deliverable 17**). The CM Plan shall outline the processes for detailed recording and updating of information related to hardware and software assets and

configurations for all networks. As part of the CM Plan, the contractor shall create and maintain, in real time, Operational Drawings (**Section F, Deliverable 26**) of logical and physical configuration and topographies for the AO Uniform.

C.5.8.7 SUBTASK 8.7 – ASSET MANAGEMENT

The contractor shall provide engineering, implementation, and O&M of an automated, real-time, Asset Management and Tracking System (**Section F, Deliverable 18**) capable of tracking all of USSOUTHCOM's IT equipment and ancillary support equipment. This includes, but is not limited to, tracking the make, model, serial number, asset tag number, accountability, location, acquisition date, associated acquisition data, receiving date, warranty information, anticipated lifecycle date, and disposition. The contractor shall also perform asset management through additional required systems of asset management, including, but not limited to, USSOUTHCOM Property Book Office systems and Department of the Army (DA) systems.

The contractor shall maintain a software library of all supported software on the enterprise. Software shall be tracked in the asset management software. Software shall be maintained in both digital form and original format, including, but not limited to, digital file, optical media, and hardware tokens. All associated Access Information Log (**Section F, Deliverable 27**) information, including, but not limited to, passwords, tokens, logins, information, support contracts, expiration dates of contracts, and per-user costs. The contractor shall inform USSOUTHCOM no less than 60 days prior to the expiration of license or support contracts.

C.5.8.8 SUBTASK 8.8 – LIFECYCLE MANAGEMENT

The contractor shall provide IT lifecycle procurement planning and execution activities. The contractor shall monitor the procurement of IT lifecycle commodities to ensure they align with the Government's guidance and approval. The contractor shall perform the planning and execution for all lifecycle activities, maintain lists of all hardware and software, and identify what systems and components are due for lifecycle updates in the MSR (**Section F, Deliverable 04**).

C.5.8.9 SUBTASK 8.9 – FACILITIES EQUIPMENT MANAGEMENT

The contractor shall provide facilities monitoring and reporting of all USSOUTHCOM communications facilities including, but not limited to, water intrusions sensors, Heating, Ventilation, and Air Conditioning (HVAC) system operations, environmental conditions, and power systems. The contractor shall provide installation, engineering, and O&M of facilities equipment including, but not limited to, generators, HVAC systems, Uninterruptible Power Supplies (UPS), and power distribution units.

C.5.8.10 SUBTASK 8.10 – SPECIAL EVENTS AND EXERCISE SERVICES

The contractor shall provide logistical services as needed for local training exercises, workshops, conferences, special events, and VIP events. The contractor shall provide services, along with Government staff, for roughly 170 of these events in the Base Period. In future periods, the Government anticipates that the annual number of events will increase by 10 percent, on average, year over year. These special event and exercise services include, but are not limited to, IT equipment deployment (shipping/receiving, setup, cabling, and configuration) and on-site event

services (room configuration, live A/V, and voice and data connectivity) at local and remote locations.

C.5.9 TASK 9 – ADDITIONAL USSOUTHCOM CYBER INFORMATION TECHNOLOGY ENTERPRISE SERVICES (SCITES) AUGMENTED SERVICES (OPTIONAL)

Unpredictable world events require that USSOUTHCOM have the capability to provide reach-back for additional augmented SCITES services to combat threats and conduct USSOUTHCOM activities in emergent situations. The contractor shall provide additional SCITES augmented services when directed by the FEDSIM Contracting Officer at any point during the TO performance, in accordance with the terms and conditions of this TO. The contractor shall provide additional augmented services for any requirement in Section C.5 that is within the scope of the TO. These events may be in conjunction with other USG and DoD organizations as a result of USSOUTHCOM activities. The contractor shall meet and maintain requirements identified by the USSOUTHCOM TPOC and the FEDSIM COR during events of contingency, training situations, or wartime in order to service directed expansion planning, exercises, and operations when required by USSOUTHCOM.

When the requirement for additional SCITES augmented services is identified, the FEDSIM CO and/or FEDSIM COR will notify the contractor in advance and exercise the optional additional augmented services. The additional augmented services shall not result in a decrease of services to other TO requirements unless approved by the FEDSIM CO and/or FEDSIM COR.

The following applies to the performance of SCITES additional augmented services:

a. The Government will determine the amount of additional SCITES augmented services required at the time of the crisis action matter. Each crisis action matter may require a different amount and length of augmented services.
b. The contractor shall provide additional SCITES augmented services in response to identified crisis action matters with the urgency the matter entails. Additional SCITES augmented services shall be staffed and worked within USSOUTHCOM spaces, following the first notification informing the contractor of a request for additional augmented services.

Once a crisis action matter has been declared ended or the additional augmented services are no longer needed, the contractor shall proceed with an orderly and efficient transition-out period NTE 30 calendar days. During the transition-out period, the contractor shall fully cooperate with, and assist the Government with, activities closing out the crisis action matter, developing required documentation, transferring knowledge, and documenting lessons learned in an Augmented Services Transition-Out Plan (**Section F, Deliverable 11**). The contractor shall also be prepared to extend its service hours to include evenings and weekends when required by the Government (e.g., real-world missions, contingences and exercises, and other customer requirements).